Mini Guía para usar las Keops en el ITAM

Adrián Puente Z. Sala de Servidores Instituto Tecnológico Autónomo de México

7 de abril de 2005

1. Introducción.

Cómo alumno de la materia de Sistemas Operativos he visto la necesidad de los alumnos de poder emplear las máquinas de Keops para poder hacer sus prácticas de UNIX. Por seguridad estas máquinas se encuentran detrás de un Firewall aparte de que los servicios de FTP y Telnet son extremadamente inseguros por transferir los datos en texto plano.

Con esta guía busco ayudar a los alumnos para facilitarle la manera de hacer sus prácticas y que aprenda un nuevo concepto cómo el tuneleo y el protocolo de SSH.

2. Algunos conceptos.

Es un protocolo que vino a sustituir el protocolo de telnet, rlogin y rsh que mostraron ser inseguros al transferir los datos de forma de texto plano que puede ser capturada con cualquier analizador de protocolos que se encuentre en la red (ataque de hombre en medio).

Este protocolo funciona con un intercambio de llaves formando un "túnel" de cifrado que sólo los poseedores de las llaves puedan accesar al contenido de el túnel. Este protocolo es muy dinámico, aparte de darnos una sesión interactiva de shell, también podemos transferir archivos y redirecciona puertos de otras máquinas permitiendo crear "túneles" para aplicaciones que son menos seguras.

Para esto un ejemplo:

Digamos que somos la máquina usuario y queremos accesar a la keops12.itam.mx por telnet desde nuestra casa. Obviamente no podemos por el Firewall instalado entre nosotros y la máquina keops12.itam.mx. Por otro lado tenemos la máquina alumnos.itam.mx de la cual tenemos un usuario válido y este nos da servicio de SSH y podemos alcanzarlo desde nuestra casa pues el Firewall tiene abierto ese puerto para la máquina alumnos.itam.mx.



Si usamos las propiedades que nos brinda este protocolo podemos crear un túnel seguro para poder accesar al puerto de Telnet de la máquina keops12 pasando a través de la máquina Shell. En pocas palabras vamos a conectarnos desde nuestra máquina a la máquina alumnos.itam.mx usando el protocolo de Secure Shell (puerto 22) para redirigirlo. Por ende podemos concluir que usamos la máquina servidor de SSH cómo Proxi para ingresar a servicios de otras máquinas que están bloqueadas por seguridad.

3. Menos charla mas acción.

Para lograr esto en Windows necesitamos un cliente de Secure Shell que podemos descargar aquí http://www.chiark.greenend.org.uk/~sgtatham/putty/

Este funcional cliente aparte de que es pequeño, es cliente de Telnet y Secure Shell. empecemos con la configuración. Para lograr un Proxi de SSH tenemos que asignar un puerto local, el nombre o IP de la máquina a la que queremos accesar y el puerto remoto. El puerto local es en el cual nos hemos de conectar y que estará ligado con el túnel SSH al Proxi que nos redirigirá al puerto de la máquina remota.

Abrimos el	programa	de Putty	y nos	vamos	a la	sección	detúr	ieles	casi	hasta
el final de las	opciones.									

	Options controlling SSH tunnel	ling		
Logging	X11 forwarding	860		
 Terminal Keyboard 	Enable X11 forwarding			
Bel	Port forwarding			
E-Window Appearance Behaviour Translation				
Selection	Forwarded ports:	Bemove		
E-Connection Proxy Teinet	L2301 keops12.itam.mx. L2302 keops12.itam.mx.	23 23		
- Proxy Teinet				
⊢ Proxy Teinet ⊢ Riogin ⊡ SSH	Add new forwarded port:			
Proxy Teinet Riogin ⊟ SSH Auth	Add new forwarded port:	Add		
Proxy Teihet Riogin ⊡ SSH Auth Tunnels	Add new forwarded port Source port 2303 Destination keops12.item	Add mx23		

El source port es nuestro puerto local, al que vamos a conectarnos al túnel para hacer Telnet en este caso. El destino es la máquina con el puerto al que queremos conectarnos. Ahora debemos ingresar a las opciones que nos den la conexión al Proxi.

Basic options for your PuTTY session Specify your connection by host name or IP address				
Host Name (or IP address)	Port			
alumnos. kam.mx	22			
Protocol C Baw C Ielnet C Blogin	• ISSH			
Load, save or delete a stored session Saved Sessions				
Keops12 2301-2302 telnet				
Default Settings Kersel 2 2201 2302 telest	Load			
Neups 12 2301-2302 (Shiel	Saye			
	Delete			
Close window on ext				
	Basic options for your PuTTY session Specify your connection by host name or Host Name (or IP address) [alumnos.kam.mx Protocol Plaw I lenet Riogn Load, save or delete a stored session Saved Sessions [Keops12 2301-2302 telnet Default Settings Keops12 2301-2302 telnet Close window on est			

Podemos guardar nuestra configuración con un nombre bastante sugerente. En mi caso decidí usar los puertos 2301 y 2302 por varias razones, entre ellas que muchas veces se necesitan ciertos privilegios para abrir puertos de escuchar menores a 1024, porque 2301 me recuerda que es el puerto remoto 23 túnel 01 ya que para cada conexión hay que hacer un túnel diferente y cada túnel usa un puerto local. Ok, ingresamos el servidor que nos servirá de Proxi usando el protocolo de SSH. y nos conectamos. Este es el servidor de correo del ITAM. Todos los alumnos tienen cuenta en el y si no, lo pueden solicitar en el SYTI del ITAM. En fin, ingresamos nuestro usuario y contraseña válidos y ya que entremos al servicio podemos minimizar la pantalla pues con ella ya no haremos nada mas que usar los túneles que ha creado.

Selection	inar C: WINNT, System 32 cm	Lenne .		- IDI XI
CINOnets	tat -an			
Convertion	ant antions			
citite a anti-	na atsayaa			1.12
Frata	Dirección local	Direction remate	Estado	
ICP	0.0.0.01135	8.8.8.910	LISTENING	
ICP	0.0.0.01445	020202010	LISTENING	
TCP	0.0.0.011025	8.8.8.919	LISTENING	
TCP	0.0.0.011027	.0.0.0.010	LISTENING	
ICP	0.0.0.011057	010101010	LISTENING	
TCP	0.0.0.0)2181	010101010	LIBTENING	
TOP	0.0.0.0:2186	8.8.8.818	LISTENING	
TCP	0.0.0.0:5800	.0.0.0.00	LISTENING	
TCP	0:0:0:0:5780	010101010	LISTENING	
TCP	0.0.0.019104	0.0.0.010	LISTENING	
TCP	0.0.0.0:31819	0.0.0.010	LISTENING	
TCP	0.0.0.0142510	0.0.0.010	LISTENING	1 A A A A A A A A A A A A A A A A A A A
ICP	127.8.8.1 (238)	0.0.0.010	LISTENING	202
ICP	127.0.0.112302	0.0.0.010	LISTENING	
TCP	192.168.1.111139	0.0.0.0:0	LISTENING	
TCP	192.168.1.1111857	12.129.285.228188	ESTABLISHED	
TOP	192.168.1.11 2101	148.265.132.14/22	ESTRELIENCE	
TCP	192.168.1.1115988	192.168.1.13132829	ERTABLICHED	
- U.B#	0.0.0.0:135			
UDP .	0.0.0.01445			+

Si ejecutamos el comando netstat -an podemos ver cómo los puertos 2301 y el 2302 están abiertos en nuestra máquina y esperan conexión, misma que haremos con nuestro cliente de telnet.

E Session	Basic options for your PuTTY session	
 Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Proxy Telnet Riogin SSH Auth Tunnels Bugs 	Specify your connection by host name or Host Name (or IP address) [localhost] Protocot ○ Baw	IP address <u>Port</u> 2301
	Load, save or delete a stored session Saved Sessions Detaut Settings Keops12 2301-2302 tenet	Load Saye Delete
	Close window on exit. Always Never P Only on	clean exit

Abrimos nuevamente nuestro cliente putty y ahora nos conectamos localmente al puerto que tiene el túnel, en mi caso es el 2301, usando el protocolo Telnet que es el que queremos usar para la keops12.itam.mx.



Cómo podemos ver el cliente putty se conecta localmente (mi máquina se llama Artemisa) pero vemos el login de la deseada keops12.itam.mx. En pocas palabras estamos haciendo un túnel SSH a la máquina alumnos.itam.mx y este nos redirige el contenido del túnel, en este caso la conexión telnet, a la máquina keops02.itam.mx.

4. Conclusiones.

SSH ha demostrado ser un protocolo muy dinámico, poderoso y seguro pues aparte de darnos privacidad de la información que estamos transmitiendo, nos da autenticación pues maneja huellas digitales de la llave RSA que empleamos y nos solicitarnos usuario y contraseña para ingresar al sistema y no repudiación al quedarse logeado el ingreso del usuario. Un protocolo lindo ¿no?

Este mismo método de Proxi también puede servir para otros protocolos cómo POP3 SMTP y FTP que carga información sensible y no tienen privacidad.